

You cannot use certain Web applications that use the InfoTech protocol after you install Windows Server 2003 Service Pack 1, MS05-026, or MS04-023

Important This article contains information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. For information about how to back up, restore, and edit the registry, click the following article number to view the article in the Microsoft Knowledge Base:

[256986](#) Description of the Microsoft Windows Registry

Article ID : 896054
Last Review : June 14, 2005
Revision : 3.0

SYMPTOMS

After you install Microsoft Windows Server 2003 Service Pack (SP1), MS05-026, or MS04-023, you may experience the following symptoms:

- If you have installed Windows Server 2003 SP1 or MS05-026, you may experience the following symptoms:
 - The features of some of Web applications on the computer no longer work. For example, a topic may not display after you click a link.
 - When you try use a Universal Naming Convention (UNC) path of open a Compiled Help Module (CHM) file on a network shared folder, topics in the CHM file do not appear.
- If you have installed security update MS04-023, the Web applications on the computer that nest protocols within the InfoTech protocols within a URL do not work correctly.

CAUSE

Windows Server 2003 SP1 and security updates MS05-026 and MS04-023 include changes to the InfoTech protocol. These changes were introduced to reduce security vulnerabilities in HTML Help.

RESOLUTION

Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

To resolve these problems, you must modify the ItssRestrictions registry entry in the registry of the computer. The ItssRestrictions registry entry supports the various capabilities of the InfoTech protocol.

Consumers and non-enterprise customers

To modify the ItssRestrictions registry entry, use one of the following methods, depending on which capabilities of the InfoTech protocol you want to enable.

Method 1: Modify the ItssRestrictions registry entry to enable a specific Web application

Warning Enable only those Web applications that you trust. Do not enable Web applications about which you are not sure.

To modify the ItssRestrictions registry entry to enable a specific Web application, follow these steps:

1. Click Start, click Run, type regedit , and then click OK.
2. Locate and then click the following subkey:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions

Note If this registry subkey does not exist, create it. To do this, follow these steps:

- a. On the Edit menu, point to New, and then click Key.
 - b. Type ItssRestrictions, and then press ENTER.
3. Right-click the ItssRestrictions subkey, point to New, and then click String Value.
 4. Type UriAllowList, and then press ENTER.
 5. Right-click the UriAllowList value, and then click Modify.
 6. In the Value data box, type the name of the Web application that you want to enable, and then click OK.

Notes

- Entries in the UriAllowList value are separated by a semicolon. If you want to enable more than one Web application,

you must separate the entries with a semicolon, as in the following example:

`http://www.wingtip toys.com/help/helpdocuments;http://contoso/help/helpfiles`

- If you want to enable a UNC path to a network shared folder, you must add two entries, as in the following example:

`\\<servername>\helpfiles\;file://\\<servername>\helpfiles`

7. Quit Registry Editor.

Note The use of wildcard characters within the URL string of any site that is being added to the `UrlAllowList` registry key does not work and is not supported. For example, "`UrlAllowList`"="`http://*.wingtip toys.com`" does not work. However, "`UrlAllowList`"="`http://help.wingtip toys.com`" succeeds, and would allow the system to connect to sites such as `http://help.wingtip toys.com/research` and `http://help.wingtip toys.com/sales` by using the InfoTech protocol.

Method 2: Modify the `ItssRestrictions` registry entry to enable a specific security zone

Warning Enable only those security zones that you trust. Do not enable security zones about which you are not sure.

To modify the `ItssRestrictions` registry entry to enable a specific security zone, follow these steps:

1. Click Start, click Run, type `regedit`, and then click OK.
2. Locate and then click the following subkey:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions`

Note If this registry subkey does not exist, create it by using Steps 2a and 2b in Method 1.

3. Right-click the `ItssRestrictions` subkey, point to New, and then click `DWORD Value`.
4. Type `MaxAllowedZone`, and then press ENTER.
5. Right-click the `MaxAllowedZone` value, and then click Modify.
6. In the Value data box, type a number from 0 and 4, and then click OK.
7. Quit Registry Editor.

Note By default, the `MaxAllowedZone` value is set to zero. The following table summarizes how different entries are interpreted by the `MaxAllowedZone` value.

<code>MaxAllowedZone</code>	Local Machine zone	Local intranet zone	Trusted sites zone	Internet zone	Restricted sites zone
0	Allowed	Blocked	Blocked	Blocked	Blocked
1	Allowed	Allowed	Blocked	Blocked	Blocked
2	Allowed	Allowed	Allowed	Blocked	Blocked
3	Allowed	Allowed	Allowed	Allowed	Blocked
4	Allowed	Allowed	Allowed	Allowed	Allowed

For more information about how to use security zones in Internet Explorer, click the following article number to view the article in the Microsoft Knowledge Base:

[174360](#) How to use security zones in Internet Explorer

Method 3: Modify the `ItssRestrictions` registry entry to enable nested protocols within a URL

Certain Web applications may use nested protocols within a URL. This feature was removed from HTML Help with the MS04-023 security update. After you install the MS04-023 security update, Web applications that use nested protocols within a URL will not work correctly.

To resolve this problem, you must modify the `ItssRestrictions` registry entry to enable nested protocols within a URL. To do this, follow these steps:

1. Click Start, click Run, type `regedit`, and then click OK.
2. Locate and then click the following subkey:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions`

Note If this registry subkey does not exist, create it by using Steps 2a and 2b in Method 1.

3. Right-click the NestedProtocolList value, and then click Modify.

Note If this registry subkey does not exist, create it. To do this, follow these steps:

- a. Right-click the ItssRestrictions subkey, point to New, and then click String Value.
- b. Type NestedProtocolList, and then press ENTER.
- c. Right-click the NestedProtocolList value, and then click Modify.

4. In the Value data box, type the protocols that you want to enable, and then click OK.

Note Entries in the NestedProtocolList value are separated by a semicolon. If you want to enable more than one protocol, separate the entries with a semicolon, as in the following example:

http;ftp

This method lets you nest the http and ftp protocols within a URL, as in the following example: ms-its:http://www.proseware.com/helpfiles/help.chm::about.htm

5. Quit Registry Editor.

Note If you modify the ItssRestrictions registry entry to enable nested protocols within a URL, you must also modify the ItssRestrictions registry entry to enable specific Web applications, by using UrlAllowList, or security zones, by using MaxAllowedZone.

For more information about the MS04-023 security update, click the following article number to view the article in the Microsoft Knowledge Base:

[840315](#) Vulnerability in HTML Help could allow code execution

Enterprise customers

To modify the ItssRestrictions registry entry across a domain by using Group Policy, use one of the following methods, depending on which capabilities of the InfoTech protocol you want to enable.

Method 1: Modify the ItssRestrictions registry entry to enable a specific Web application

Warning Enable only those Web applications that you trust. Do not enable Web applications about which you are not sure.

To modify the ItssRestrictions registry entry to enable a specific Web application, follow these steps:

1. Copy the following text, and then paste the text into a text editor, such as Notepad:

```
REGEDIT4 ["HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions\UrlAllowList"=String: the name of the Web application that you want to enable
```

Notes

- Entries in the UrlAllowList value are separated by a semicolon. If you want to enable more than one Web application, you must separate the entries with a semicolon, as in the following example:

http://www.wingtip toys.com/help/helpdocuments;http://contoso/help/helpfiles

- If you want to enable a UNC path of a network shared folder, you must add two entries, as in the following example:

\\<servername>\helpfiles\;file://\<servername>\helpfiles

2. Save the file as "UrlAllowList.reg".
3. Copy the following text, and then paste the text into a text editor, such as Notepad:

```
REGEDIT.EXE /S UrlAllowList.reg
```

4. Save the file as "UrlAllowList.bat".

Note Before you deploy the batch file, make sure that the batch file works correctly by testing it on one computer.

5. Import the batch file into the Group Policy object (GPO). To do this, follow these steps:

- a. Copy the UrlAllowList.bat file and the UrlAllowList.reg file to the \\DomainName\SysVol\DomainName\Policies\GUID folder of the selected GPO\Machine\Scripts\Startup folder.
- b. Start the Active Directory Users and Computers tool on a domain controller. To do this, click Start, click Run, type dsa.msc , and then click OK.
- c. Right-click the domain, click Properties, and then click the Group Policy tab.
- d. Click New, type a descriptive name for the new Group Policy object (GPO), and then press ENTER. For example, click New, type UrlAllowList, and then press ENTER.
- e. Click Edit to modify the new GPO that you created in step 5d.
- f. Expand Computer configuration, expand Windows Settings, click Scripts(Startup/Shutdown), click Startup, and then click Add.
- g. Locate and then click the batch file that you created in step 4, and then click Add.
- h. Click OK, click Yes, and then click OK two times.

Note The use of wildcard characters within the URL string of any site that is being added to the UrlAllowList registry key does not work and is not supported. For example, "UrlAllowList"="http://*.wingtiptoy.com" does not work. However, "UrlAllowList"="http://help.wingtiptoy.com" succeeds, and would allow the system to connect to sites such as http://help.wingtiptoy.com/research and http://help.wingtiptoy.com/sales by using the InfoTech protocol.

Method 2: Modify the ItssRestrictions registry entry to enable a specific security zone

Warning Enable only those security zones that you trust. Do not enable security zones about which you are not sure.

To modify the ItssRestrictions registry entry to enable a specific security zone, follow these steps:

1. Copy the following text, and then paste it into a text editor, such as Notepad:

```
REGEDIT4
["HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions\MaxAllowedZone"]=DWORD: a number from 0 to 4
```

2. Save the file as "MaxAllowedZone.reg".
3. Copy the following text, and then paste it into a text editor, such as Notepad:

```
REGEDIT.EXE /S MaxAllowedZone.reg
```

4. Save the file as "MaxAllowedZone.bat".

Note Before you deploy the batch file, make sure that the batch file works correctly by testing it on one computer.

5. Import the batch file into the GPO. To do this, follow these steps:
 - a. Copy the MaxAllowedZone.bat file that you created in step 4 and the MaxAllowedZone.reg file to the \\DomainName\SysVol\DomainName\Policies\GUID of the selected GPO\Machine\Scripts\Startup folder.
 - b. Start the Active Directory Users and Computers snap-in. To do this, click Start on a domain controller, click Run, type dsa.msc , and then click OK.
 - c. Right-click the domain, click Properties, and then click the Group Policy tab.
 - d. Click New, type a descriptive name for the new Group Policy object (GPO), and then press ENTER. For example, click New, type MaxAllowedZone, and then press ENTER.
 - e. Click Edit to modify the new GPO that you created in step 5d.
 - f. Expand Computer configuration, expand Windows Settings, click Scripts(Startup/Shutdown), click Startup, and then click Add.
 - g. Locate and then click the batch file that you created in step 4, and then click Add.
 - h. Click OK, click Yes, and then click OK two times.

Note By default, the MaxAllowedZone value is set to zero. The following table summarizes how different entries are interpreted by the MaxAllowedZone value.

MaxAllowedZone	Local Machine zone	Local intranet zone	Trusted sites zone	Internet zone	Restricted sites zone
0	Allowed	Blocked	Blocked	Blocked	Blocked

1	Allowed	Allowed	Blocked	Blocked	Blocked
2	Allowed	Allowed	Allowed	Blocked	Blocked
3	Allowed	Allowed	Allowed	Allowed	Blocked
4	Allowed	Allowed	Allowed	Allowed	Allowed

For more information about how to use security zones in Internet Explorer, click the following article number to view the article in the Microsoft Knowledge Base:

[174360](#) How to use security zones in Internet Explorer

Method 3: Modify the ItssRestrictions registry entry to enable nested protocols within a URL

Certain Web applications may use nested protocols within a URL. This feature was removed from HTML Help with the MS04-023 security update. After you install the MS04-023 security update, Web applications that use nested protocols within a URL will not work correctly.

To resolve this problem, modify the ItssRestrictions registry entry to enable nested protocols within a URL. To do this, follow these steps:

- Copy the following text, and then paste it into a text editor, such as Notepad:


```
REGEDIT4 ["HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions\NestedProtocolList"=String:
the protocol that you want to enable
```

Note Entries in the NestedProtocolList value are separated by a semicolon. If you want to enable more than one protocol, separate the entries with a semicolon, as in the following example:

```
http;ftp
```

This method lets you nest the HTTP and FTP protocols within a URL, as in the following example:

```
ms-its:http://www.proseware.com/helpfiles/help.chm::about.htm
```
- Click File, click Save, type NestedProtocolList.reg in the File name box, and then click Save.
- Copy the following text, and then paste it into a text editor, such as Notepad:


```
REGEDIT.EXE /S NestedProtocolList.reg
```
- Click File, click Save, type NestedProtocolList.bat in the File name box, and then click Save. Note Before you deploy the batch file, make sure that the batch file works correctly by testing it on one computer.
- Import the batch file into the GPO. To do this, follow these steps:
 - Copy the NestedProtocolList.bat file that you created in step 4 and the NestedProtocolList.reg file to the \\DomainName\SysVol\DomainName\Policies\GUID of the selected GPO\Machine\Scripts\Startup folder.
 - Start the Active Directory Users and Computers snap-in. To do this, click Start on a domain controller, click Run, type dsa.msc , and then click OK.
 - Right-click the domain, click Properties, and then click the Group Policy tab.
 - Click New, type a descriptive name for the new GPO, and then press ENTER. For example, click New, type MaxAllowedZone, and then press ENTER.
 - Click Edit to modify the new GPO that you created in step 5d.
 - Expand Computer configuration, expand Windows Settings, click Scripts(Startup/Shutdown), click Startup, and then click Add.
 - Locate and then click the batch file that you created in step 4, and then click Add.
 - Click OK, click Yes, and then click OK two times.

Note If you modify the ItssRestrictions registry entry to enable nested protocols within a URL, you must also modify the ItssRestrictions registry entry to enable specific Web applications, by using UrlAllowList, or security zones, by using MaxAllowedZone.

For more information about security update MS04-023, click the following article number to view the article in the Microsoft Knowledge Base:

[840315](#) MS04-023: Vulnerability in HTML Help could allow code execution

MORE INFORMATION

The InfoTech protocol is primarily used by HTML Help. The functionality of this protocol is provided by the Itss.dll file. You can access this protocol by using one of the following supported protocols:

- ms-its
- its
- mk:@msitstore

For more information about Group Policy (GPO), visit the following Microsoft Web sites:

- Group Policy Collection:
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/6d7cb788-b31d-4d17-9f1e-b5ddaa6deecd.mspx>
- What Is Group Policy Object Editor:
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/47ba1311-6cca-414f-98c9-2d7f99fca8a3.mspx>
- Core Group Policy Tools and Settings:
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/e926577a-5619-4912-b5d9-e73d4bdc9491.mspx>

APPLIES TO

- Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003, Datacenter Edition for Itanium-based Systems
- Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
- Microsoft Windows Server 2003, Enterprise x64 Edition
- Microsoft Windows Server 2003, Standard x64 Edition
- Microsoft Windows Server 2003, Datacenter x64 Edition
- Microsoft Windows 2000 Advanced Server SP3
- Microsoft Windows 2000 Advanced Server SP4
- Microsoft Windows 2000 Service Pack 3
- Microsoft Windows 2000 Datacenter Server SP4
- Microsoft Windows 2000 Service Pack 3
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows 2000 Service Pack 3
- Microsoft Windows 2000 Server SP4
- Microsoft Windows XP Service Pack 1
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional 64-Bit Edition (Itanium) 2003
- Microsoft Windows XP Professional 64-Bit Edition (Itanium)
- Microsoft Windows 98 Standard Edition
- Microsoft Windows 98 Second Edition
- Microsoft Windows Millennium Edition

Keywords: kbhowto kbtshoot kbhtmlhelp100fix kbprb KB896054
